D-23

DURIE TANGRI LLP
SONAL N. MEHTA (SBN 222086)
smehta@durietangri.com
JOSHUA H. LERNER (SBN 220755)
jlerner@durietangri.com
LAURA E. MILLER (SBN 271713)
lmiller@durietangri.com
CATHERINE Y. KIM (SBN 308442)
ckim@durietangri.com
ZACHARY G. F. ABRAHAMSON (SBN 310951)
zabrahamson@durietangri.com
217 Leidesdorff Street
San Francisco, CA 94111
Telephone: 415-362-6666
Facsimile: 415-236-6300

Attorneys for Defendants
Facebook, Inc., Mark Zuckerberg, Christopher Cox, Javier Olivan, Samuel Lessin, Michael Vernal, and Ilya Sukhar

SUPERIOR COURT OF THE STATE OF CALIFORNIA

COUNTY OF SAN MATEO

SIX4THREE, LLC, a Delaware limited liability company,

Plaintiff,

v.

FACEBOOK, INC., a Delaware corporation; MARK ZUCKERBERG, an individual; CHRISTOPHER COX, an individual; JAVIER OLIVAN, an individual; SAMUEL LESSIN, an individual; MICHAEL VERNAL, an individual; ILYA SUKHAR, an individual; and DOES 1-50, inclusive,

Defendants.

Case No. CIV 533328

Assigned for all purposes to Hon. V. Raymond Swope, Dept. 23

DECLARATION OF ZACHARY G. F. ABRAHAMSON IN SUPPORT OF REPLY TO DEFENDANT FACEBOOK, INC.'S MOTION TO OPEN DISCOVERY AND TO COMPEL

Date: March 15, 2019
Time: 10:00 a.m.
Dept: 23 (Complex Civil Litigation)
Judge: Honorable V. Raymond Swope

FILING DATE: April 10, 2015
TRIAL DATE: April 25, 2019

I, Zachary G. F. Abrahamson, declare as follows:

1. I am an attorney at law licensed to practice in the state of California. I am an attorney with the law firm of Durie Tangri LLP, counsel for Defendant Facebook, Inc. in this matter. I make this Declaration from personal knowledge, and if called to testify, I could and would testify competently thereto.

2. Attached hereto as **Exhibit 1** is a true and correct copy of the Declaration of David S. Godkin in Response to CMO No. 19, served in this matter on March 5, 2019.

3. Attached hereto as **Exhibit 2** is a true and correct copy of a March 5, 2019 letter to Sonal Mehta from Ravi Naik of Irvine Thanvi Natas Solicitors, counsel for non-party Paul-Olivier Dehaye. Attached to said letter were an engagement letter from Birnbaum & Godkin, LLP to Mr. Dehaye dated May 14, 2018; a copy of the Stipulated Protective Order entered in this matter with the Certification executed by Mr. Dehaye; and a January 8, 2019 *Financial Times* article entitled "Data brokers: regulators try to rein in the 'privacy deathstars.'"

I declare under penalty of perjury under the laws of the State of California that the foregoing is to the best of my knowledge and belief true and correct.

Executed on March 6, 2019 in San Francisco, California.

ZACHARY G. F. ABRAHAMSON

PROOF OF SERVICE

I am employed in San Francisco County, State of California, in the office of a member of the bar of this Court, at whose direction the service was made. I am over the age of eighteen years, and not a party to the within action. My business address is 217 Leidesdorff Street, San Francisco, CA 94111.

On March 6, 2019, I served the following documents in the manner described below:

DECLARATION OF ZACHARY G. F. ABRAHAMSON IN SUPPORT OF REPLY TO DEFENDANT FACEBOOK, INC.'S MOTION TO OPEN DISCOVERY AND TO COMPEL

[X] BY ELECTRONIC SERVICE: By electronically mailing a true and correct copy through Durie Tangri's electronic mail system from cortega@durietangri.com to the email addresses set forth below.

On the following part(ies) in this action:

Stuart G. Gross
GROSS & KLEIN LLP
The Embarcadero, Pier 9, Suite 100
San Francisco, CA 94111
sgross@grosskleinlaw.com

David S. Godkin
James Kruzer
BIRNBAUM & GODKIN, LLP
280 Summer Street
Boston, MA 02210
godkin@birnbaumgodkin.com
kruzer@birnbaumgodkin.com

Attorneys for Plaintiff Six4Three, LLC

Donald P. Sullivan
Wilson Elser
525 Market Street, 17th Floor
San Francisco, CA 94105
donald.sullivan@wilsonelser.com
Joyce.Vialpando@wilsonelser.com
Dea.Palumbo@wilsonelser.com

Attorney for Gross & Klein LLP

Jack Russo
Christopher Sargent
ComputerLaw Group, LLP
401 Florence Street
Palo Alto, CA 94301
jrusso@computerlaw.com
csargent@computerlaw.com
ecf@computerlaw.com

Attorney for Theodore Kramer and Thomas Scaramellino (individual capacities)

Steven J. Bolotin
Morrison Mahoney LLP
250 Summer Street
Boston, MA 02210
sbolotin@morrisonmahoney.com
Llombard@morrisonmahoney.com

James A. Murphy
James A. Lassart
Thomas P Mazzucco
Joseph Leveroni
Murphy Pearson Bradley & Feeney
88 Kearny St, 10th Floor
San Francisco, CA 94108
JMurphy@MPBF.com
jlassart@mpbf.com
TMazzucco@MPBF.com
JLeveroni@MPBF.com

Attorney for Birnbaum & Godkin, LLP

I declare under penalty of perjury under the laws of the United States of America that the foregoing is true and correct. Executed on March 6, 2019, at San Francisco, California.

Christina Ortega

EXHIBIT 1

Conditionally Lodged Under Seal in its Entirety

EXHIBIT 2

ITN
SOLICITORS

19-21 Great Tower Street
Tower Hill
London, EC3R 5AQ

Stratford Office:
City View House
1 Dorset Place
Stratford City
London, E15 1BZ

T: 020 3909 8100
F: 020 3929 3332

DX: 307450 Cheapside

enquiries@itnsolicitors.com
www.itnsolicitors.com

Sonal N. Mehta
Durie Tangri

By email: smehta@durietangri.com

05 March 2019

Our ref: RAN/32411

Dear Ms Mehta

Paul-Olivier Dehaye

We have been instructed to represent the above named.

Our client has received correspondence from David Godkin of Birnbaum & Godkin, LLP relating to *Six4Three v Facebook Inc. et al.*

On 1 March 2019, Mr Godkin provided Mr Dehaye with an order from the Superior Court of California explaining that our client was required to provide a declaration to the court by 17:00 Eastern Time on 5 March 2019. Mr Godkin did not provide the background documents to that order until 20:00 GMT on 4 March 2019, after a request for those documents from this firm.

Having considered those documents, we are instructed to write to you to provide some clarity to our client's role in the *Six4Three* litigation as there appears to be a misunderstanding of his role and his retainer. You will appreciate that our client has been cut out from the process to date, which has prejudiced his ability to explain his role and the basis for his limited involvement in the case.

1. Our client's background

Mr Dehaye is a well-known privacy and data rights activist. He is renowned for his insight into the European data protection regime, as well as his capacity to convey such subjects to a wider audience.

He has been regularly sought for commentary and insight in the media in this role. This includes commentary in the *Financial Times,* the *Economist*, *ProPublica* and *WIRED* amongst many others. We enclose examples of that commentary for your client's consideration, which demonstrate Mr Dehaye's unique ability to humanise complex technical issues and to explain the importance of the data protection regime as a matter of wider public interest.

2. Our client's role with *Six4Three*

In the context of that expertise, our client was approached by Mr Godkin to act as an expert on public interest elements of the *Six4Three* litigation. Mr Dehaye was provided with a letter of engagement on 14 May 2018. We enclose a copy of that engagement letter.

You will see that the terms of the retainer were not well drafted but that Mr Dehaye was retained by Birnbaum & Godkin, LLP to "assist [them] in reviewing Facebook's arguments related to digital privacy issues." This is what our client understood his role to be and acted at the instruction of Birnbaum & Godkin, LLP and their clients in this litigation. Mr Dehaye has not been paid for these services.

To be clear, Mr Dehaye is not a lawyer and was therefore reliant on Birnbaum & Godkin, LLP to understand the US process and the terms of the Protective Order.

3. Execution of the Protective Order

Mr Dehaye was provided with the Protective Order by Birnbaum & Godkin, LLP on 10 May 2018. The certificate was executed on 14 May 2018. We enclose the certified version.

Klein & Gross LLP were appointed as Mr Dehaye's agent for service of process, on the recommendation of Birnbaum & Godkin, LLP. Mr Dehaye was not provided with any independent legal advice on the terms of the order at the time it was provided to him nor when it was executed.

4. Current status of documents

On 4 January 2019, Mr Godkin requested Mr Dehaye to destroy all confidential and highly confidential documents. Mr Godkin requested Mr Dehaye to do so, as Birnbaum & Godkin, LLP were no longer able to act for the Plaintiff.

Mr Dehaye destroyed all Facebook confidential and highly confidential information in his custody or control between 4 January 2019 and 11 January 2019.

Mr Dehaye maintained a contemporaneous record of the documents he had received, as and when he received them. Accordingly, he is able to confirm that he has deleted all the documents he had received marked "Confidential" or "Highly Confidential" under the Protective Order. These are the documents listed an Annex 1. He also received internal case summaries prepared by the Plaintiffs and has permanently deleted those documents as well.

5. Further matters

Our client is concerned by the nature of the allegations levied at him. Being kept from these proceedings has prejudiced his position by preventing him from being able to explain his limited role. For instance, page 7 line 8 of Facebook's *ex parte* application of 25 February 2019 suggests that Mr Dehaye agreed to "confirm details of the confidential

information" to reporters "anonymously." Mr Dehaye denies having said the same and has not been provided with the document referred to. He is unaware of any such email and should it exist, please provide it to Mr Dehaye through this firm.

We trust that the information provided with this letter and enclosures clarifies the position for Facebook and quells any further concerns your client may have. We should be grateful if you could provide a copy of this letter to the court and the Honorable Judge V. Raymond Swope accordingly.

Should you have any queries in respect of this matter please contact Mr Ravi Naik of our offices.

Yours faithfully

Irvine Thanvi Natas Solicitors

cc. David Godkin, Birnbaum & Godkin, LLP

Annex 1: Documents deleted

- FB-00061249_image.pdf
- FB-00061393_image.pdf
- FB-00061614.xlsx
- FB-00089734.pdf
- FB-00089881.pdf
- FB-00109950.pdf
- FB-00109957
- FB-00423235_image.pdf
- FB-00433779_image.pdf
- FB-00434425_image.pdf
- FB-00454582.pdf
- FB-00517457.pdf
- FB-00556670.pdf
- FB-00600167.pdf
- FB-00917804.pdf
- FB-00934373.pdf
- FB-00943408.pdf
- FB-00947595.pdf
- FB-00947909.pdf
- FB-00948130.pdf
- FB-00948246.pdf
- FB-00948764.pdf
- FB-00954660.pdf
- FB-01155756.pdf
- FB-01188663.pdf
- FB-01193711.pdf
- FB-01203441.pdf
- FB-01221432.pdf
- FB-01335815.pdf

- FB-01352766.pdf
- FB-01353432.pdf
- FB-01363612.pdf
- FB-01368113.pdf
- FB-01368198.pdf
- FB-01368870.pdf
- FB-01369059.pdf
- FB-01370694.pdf
- FB-01389021.pdf
- FB-01390441.pdf

BIRNBAUM & GODKIN, LLP
ATTORNEYS AT LAW

David S. Godkin
Direct Dial: (617) 307-6110
godkin@birnbaumgodkin.com

May 14, 2018

BY EMAIL ONLY (paulolivier@gmail.com)

Mr. Paul-Olivier Dehaye
Chemin des Fauvettes 18
1212 Grand-Lancy
Switzerland

Re: Six4Three, LLC v. Facebook, Inc., Civ. 533328

Dear Paul:

I am writing to confirm that Birnbaum & Godkin, LLP, as counsel for Six4Three, LLC, is engaging you as an expert consultant in the above-referenced matter to assist us in reviewing Facebook's arguments related to digital privacy issues. The initial phase of this engagement will involve your review of a brief and declaration that we have prepared in opposition to a motion to strike filed by Facebook, both of which include citations to various documents produced by Facebook in the above litigation. In addition, we will provide you with such of the Facebook documents that you request. You have agreed that you will not charge for this phase of the engagement. We will discuss compensation for later phases of the engagement, including possible testimony, and related compensation for your time, at a later date.

You agree that you will maintain in the strictest of confidence all aspects of this engagement including, but not limited to, all materials reviewed, generated or received by you or sent by you to this firm or our client. You will refrain from speaking with anyone about this matter and you will treat all communications with my client and my firm as privileged. Finally, you agree that any materials provided to you and any report that you prepare at our request shall be the property of the attorneys who have retained you and will not be used or disclosed without our consent.

I understand that you have already reviewed the Protective Order entered by the Court on October 24, 2016 and that you will sign the certification to same before we provide you with any documents. The brief and declaration that we will provide to you reference information that has been designated by Facebook as Confidential or Highly Confidential and are subject to the Protective Order. The Facebook documents that you request have also been designated by Facebook as Confidential or Highly Confidential and are subject to the Protective Order.

If this letter accurately describes our agreement, please sign the letter in the space provided and return it to me.

I look forward to working with you.

Very truly yours,

David S. Godkin

DSG/cam

AGREED AND ACCEPTED:

Paul-Olivier Dehaye

Date: May 14th 2018

EXHIBIT G

Julie E. Schwartz, Bar No. 260624
JSchwartz@perkinscoie.com
PERKINS COIE LLP
3150 Porter Drive
Palo Alto, CA 94304-1212
Telephone: 650.838.4300
Facsimile: 650.838.4350

James R. McCullagh, admitted *pro hac vice*
JMcCullagh@perkinscoie.com
PERKINS COIE LLP
1201 Third Avenue, Suite 4900
Seattle, WA 98101-3099
Telephone: 206.359.8000
Facsimile: 206.359.9000

Attorneys for Defendant
Facebook, Inc.

2-28 MJC

SUPERIOR COURT OF THE STATE OF CALIFORNIA

COUNTY OF SAN MATEO

SIX4THREE, LLC, a Delaware limited liability company,

Plaintiff,

v.

FACEBOOK, INC., a Delaware corporation and DOES 1-50, inclusive,

Defendant.

Case No. CIV533328

STIPULATED [PROPOSED] PROTECTIVE ORDER

In order to protect confidential information obtained by the parties in connection with this case, the parties, by and through their respective undersigned counsel and subject to the approval of the Court, hereby agree as follows:

Part One: Use Of Confidential Materials In Discovery

1. Any party or non-party may designate as Confidential Information (by stamping the relevant page or as otherwise set forth herein) any document or response to discovery which that party or non-party considers in good faith to contain information involving trade secrets, or

confidential business, financial, or personal information, including personal financial information about any individual or entity; information regarding any individual's or entity's banking relationship with any banking institution, including information regarding financial transactions or financial accounts, and any information regarding any individual or entity that is not otherwise available to the public, subject to protection under Rules 2.550, 2.551, 2.580, 2.585, 8.160, and 8.490 of the California Rules of Court or under other provisions of California law. Any party or non-party may designate as Highly Confidential Information (by stamping the relevant page or as otherwise set forth herein) any document or response to discovery which that party or non-party considers in good faith to contain information involving highly sensitive trade secrets or confidential business, financial, or personal information, the disclosure of which would result in the disclosure of trade secrets or other highly sensitive research, development, production, personnel, commercial, market, financial, or business information, or highly sensitive personal information, subject to protection under Rules 2.550, 2.551, 2.580, 2.585,8.160, and 8.490 of the California Rules of Court or under other provisions of California law. Where a document or response consists of more than one page, the first page and each page on which confidential information appears shall be so designated.

2. A party or non-party may designate information disclosed during a deposition or in response to written discovery as Confidential Information or Highly Confidential Information by so indicating in said responses or on the record at the deposition and requesting the preparation of a separate transcript of such material. In addition, a party or non-party may designate in writing, within thirty (30) days after receipt of said responses or of the deposition transcript for which the designation is proposed, that specific pages of the transcript and/or specific responses be treated as Confidential Information or Highly Confidential Information. Any other party may object to such proposal, in writing or on the record. Upon such objection, the parties shall follow the procedures described in Paragraph 9 below. Until the thirty (30) day period for designation has lapsed, the entirety of each deposition transcript shall be treated as Confidential Information. After the thirty (30) day period for designation has lapsed, any documents or information designated pursuant to the procedure set forth in this paragraph shall be treated according to the

designation until the matter is resolved according to the procedures described in Paragraph 9 below, and counsel for all parties shall be responsible for marking all previously unmarked copies of the designated material in their possession or control with the specified designation. A party that makes original documents or materials available for inspection need not designate them as Confidential Information or Highly Confidential Information until after the inspecting party has indicated which materials it would like copied and produced. During the inspection and before the designation and copying, all of the material made available for inspection shall be considered Highly Confidential Information.

3. All Confidential Information or Highly Confidential Information produced or exchanged in the course of this case (not including information that is publicly available) shall be used by the party or parties to whom the information is produced solely for the purpose of this case. Confidential Information or Highly Confidential Information shall not be used for any commercial competitive, personal, or other purpose. Confidential Information or Highly Confidential Information must be stored and maintained by a receiving party at a location and in a secure manner that ensures that access is limited to the persons authorized under this Stipulated Protective Order. The protections conferred by this Stipulated Protective Order cover not only the Confidential Information or Highly Confidential Information produced or exchanged in this case, but also (1) any information copied or extracted from or reflecting the Confidential Information or Highly Confidential Information; (2) all copies, excerpts, summaries, or compilations of Confidential Information or Highly Confidential Information; and (3) any testimony, conversations, or presentations by parties or their counsel that might reveal Confidential Information or Highly Confidential Information. However, the protections conferred by this Stipulated Protective Order do not cover the following information: (a) any information that is in the public domain at the time of disclosure to a receiving party or becomes part of the public domain after its disclosure to a receiving party as a result of publication not involving a violation of this Stipulated Protective Order, including becoming part of the public record through trial or otherwise; and (b) any information known to the receiving party prior to

the disclosure or obtained by the receiving party after the disclosure from a source who obtained the information lawfully and under no obligation of confidentiality to the designating party.

4. Except with the prior written consent of the other parties, or upon prior order of this Court obtained upon notice to opposing counsel, Confidential Information shall not be disclosed to any person other than:

(a) counsel for the respective parties to this litigation, including in-house counsel and co-counsel retained for this litigation;

(b) employees of such counsel;

(c) individual parties or officers or employees of a party, to the extent deemed necessary by counsel for the prosecution or defense of this litigation;

(d) consultants or expert witnesses retained for the prosecution or defense of this litigation, provided that each such person shall execute a copy of the Certification annexed to this Order (which shall be retained by counsel to the party so disclosing the Confidential Information and made available for inspection by opposing counsel during the pendency or after the termination of the action only upon good cause shown and upon order of the Court) before being shown or given any Confidential Information, and provided that if the party chooses a consultant or expert employed by the opposing party or one of its competitors, the party shall notify the opposing party, or designating non-party, before disclosing any Confidential Information to that individual and shall give the opposing party an opportunity to move for a protective order preventing or limiting such disclosure;

(e) any authors or recipients of the Confidential Information or a custodian;

(f) the Court, court personnel, and court reporters; and

(g) witnesses (other than persons described in Paragraph 4(e)). A witness shall sign the Certification before being shown a confidential document. Confidential Information may be disclosed to a witness who will not sign

the Certification only in a deposition at which the party who designated the Confidential Information is represented or has been given notice that Confidential Information produced by the party may be used. At the request of any party, the portion of the deposition transcript involving the Confidential Information shall be designated "Confidential" pursuant to Paragraph 2 above. Witnesses shown Confidential Information shall not be allowed to retain copies.

5. Except with the prior written consent of the other parties, or upon prior order of this Court obtained after notice to opposing counsel, Highly Confidential Information shall be treated in the same manner as Confidential Information pursuant to Paragraph 4 above, except that it shall not be disclosed to individual parties or directors, officers or employees of a party, or to witnesses (other than persons described in Paragraph 4(a) or 4(e)).

6. Any persons receiving Confidential Information or Highly Confidential Information shall not reveal or discuss such information to or with any person who is not entitled to receive such information, except as set forth herein. If a party or any of its representatives, including counsel, inadvertently discloses any Confidential Information or Highly Confidential Information to persons who are not authorized to use or possess such material, the party shall provide immediate written notice of the disclosure to the party whose material was inadvertently disclosed. If a party has actual knowledge that Confidential Information or Highly Confidential Information is being used or possessed by a person not authorized to use or possess that material, regardless of how the material was disclosed or obtained by such person, the party shall provide immediate written notice of the unauthorized use or possession to the party whose material is being used or possessed. No party shall have an affirmative obligation to inform itself regarding such possible use or possession.

7. In connection with discovery proceedings as to which a party submits Confidential Information or Highly Confidential Information, all documents and chamber copies containing Confidential Information or Highly Confidential Information which are submitted to the Court shall be filed with the Court in sealed envelopes or other appropriate sealed containers. On the

outside of the envelopes, a copy of the first page of the document shall be attached. If Confidential Information or Highly Confidential Information is included in the first page attached to the outside of the envelopes, it may be deleted from the outside copy. The word "CONFIDENTIAL" shall be stamped on the envelope and a statement substantially in the following form shall also be printed on the envelope:

> "This envelope is sealed pursuant to Order of the Court, contains Confidential Information and is not to be opened or the contents revealed, except by Order of the Court or agreement by the parties."

8. A party may designate as Confidential Information or Highly Confidential Information documents or discovery materials produced by a non-party by providing written notice to all parties of the relevant document numbers or other identification within thirty (30) days after receiving such documents or discovery materials. Until the thirty (30) day period for designation has lapsed, any documents or discovery materials produced by a non-party shall be treated at Confidential Information. Any party or non-party may voluntarily disclose to others without restriction any information designated by that party or nonparty as Confidential Information or Highly Confidential Information, although a document may lose its confidential status if it is made public. If a party produces materials designated Confidential Information or Highly Confidential Information in compliance with this Order, that production shall be deemed to have been made consistent with any confidentiality or privacy requirements mandated by local, state or federal laws.

9. If a party contends that any material is not entitled to confidential treatment, such party may at any time give written notice to the party or non-party who designated the material. The party or non-party who designated the material shall have twenty (20) days from the receipt of such written notice to apply to the Court for an order designating the material as confidential. The party or non-party seeking the order has the burden of establishing that the document is entitled to protection.

10. Notwithstanding any challenge to the designation of material as Confidential Information or Highly Confidential Information, all documents shall be treated as such and shall be subject to the provisions hereof unless and until one of the following occurs:

(a) the party or non-party who claims that the material is Confidential Information or Highly Confidential Information withdraws such designation in writing; or

(b) the party or non-party who claims that the material is Confidential Information or Highly Confidential Information fails to apply to the Court for an order designating the material confidential within the time period specified above after receipt of a written challenge to such designation; or

(c) the Court rules the material is not Confidential Information or Highly Confidential Information.

11. All provisions of this Order restricting the communication or use of Confidential Information or Highly Confidential Information shall continue to be binding after the conclusion of this action, unless otherwise agreed or ordered. Upon conclusion of the litigation, a party in the possession of Confidential Information or Highly Confidential Information shall within sixty (60) days either (a) return such documents to counsel for the party or non-party who provided such information, or (b) destroy such documents. Whether the Confidential Information or Highly Confidential Information is returned or destroyed, the receiving party must submit a written certification to the producing party (and, if not the same person or entity, to the designating party) by the 60 day deadline that (1) all the Confidential Information or Highly Confidential Information that was returned or destroyed, and (2) affirms that the receiving party has not retained any copies, abstracts, compilations, summaries or any other format reproducing or capturing any of the Confidential Information or Highly Confidential Information. Notwithstanding this provision, counsel are entitled to retain an archival copy of all pleadings, motion papers, trial, deposition, and hearing transcripts, legal memoranda, correspondence, deposition and trial exhibits, expert reports, attorney work product, and consultant and expert work product, even if such materials contain Confidential Information or Highly Confidential

Information. Any such archival copies that contain or constitute Confidential Information or Highly Confidential Information remain subject to this Stipulated Protective Order. The conclusion of the litigation shall be deemed to be the later of (1) dismissal of all claims and defenses in this action, with or without prejudice; and (2) final judgment herein after the completion and exhaustion of all appeals, rehearings, remands, trials, or reviews of this action, including the time limits for filing any motions or applications for extension of time pursuant to applicable law. After the conclusion of this action, this Court will retain jurisdiction to enforce the terms of this Order.

12. Nothing herein shall be deemed to waive any applicable privilege or work product protection, or to affect the ability of a party to seek relief for an inadvertent disclosure of material protected by privilege or work product protection. Any witness or other person, firm or entity from which discovery is sought may be informed of and may obtain the protection of this Order by written advice to the parties' respective counsel or by oral advice at the time of any deposition or similar proceeding.

13. In the event that any Confidential Information or Highly Confidential Information is inadvertently produced without such designation, the party or non-party that inadvertently produced the information without designation shall give written notice of such inadvertent production promptly after the party or non-party discovers the inadvertent failure to designate (but no later than fourteen (14) calendar days after the party or non-party discovers the inadvertent failure to designate), together with a further copy of the subject information designated as "CONFIDENTIAL" or "HIGHLY CONFIDENTIAL" (the "Inadvertent Production Notice"). Upon receipt of such Inadvertent Production Notice, the party that received the information that was inadvertently produced without designation shall promptly destroy the inadvertently produced information and all copies thereof, or, at the expense of the producing party or non-party, return such together with all copies of such information to counsel for the producing party and shall retain only the newly-produced versions of that information that are designated as "CONFIDENTIAL" or "HIGHLY CONFIDENTIAL." This provision is not intended to apply to any inadvertent production of any information or materials protected by

attorney-client or work product privileges, which inadvertent production is governed by Section 14 below.

14. In the event that any party or non-party inadvertently produces information that is privileged or otherwise protected from disclosure during the discovery process ("Inadvertent Production Material"), the following shall apply:

(a) Such inadvertent production or disclosure shall in no way prejudice or otherwise constitute a waiver of, or estoppel as to, any claim of attorney-client privilege, attorney work product protection, or other applicable protection in this case or any other federal or state proceeding, provided that the producing party shall notify the receiving party in writing of such protection or privilege promptly after the producing party discovers such materials have been inadvertently produced.

(b) If a claim of inadvertent production is made, pursuant to this Stipulated Protective Order, with respect to discovery material then in the custody of another party, that party shall: (i) refrain from any further examination or disclosure of the claimed Inadvertent Production Material; (ii) promptly make a good-faith effort to return the claimed Inadvertent Production Material and all copies thereof (including summaries and excerpts) to counsel for the producing party, or destroy all such claimed Inadvertent Production Material (including summaries and excerpts) and certify in writing to that fact; and (iii) not disclose or use the claimed Inadvertent Production Material for any purpose until further order of the Court expressly authorizing such use.

(c) A party may move the Court for an order compelling production of the Inadvertent Production Material on the ground that it is not, in fact, privileged or protected. The motion shall be filed under seal and shall not assert as a ground for entering such an order the fact or circumstance of the inadvertent production. The producing party retains the burden of establishing the privileged or protected nature of any inadvertently disclosed or produced information. While such a motion is pending, the Inadvertent Production Material at issue shall be treated in accordance with Paragraph 14(b) above.

(d) If a party, in reviewing discovery material it has received from any other party or any non-party, finds anything the reviewing party believes in good faith may be Inadvertent Production Material, the reviewing party shall: (i) refrain from any further examination or disclosure of the potentially Inadvertent Production Material; (ii) promptly identify the material in question to the producing party (by document number or other equally precise description); and (iii) give the producing party seven (7) days to respond as to whether the producing party will make a claim of inadvertent production. If the producing party makes such a claim, the provisions of Paragraphs 14(a)-(c) above shall apply.

15. The parties agree that should the production of source code become necessary, they will need to amend or supplement the terms of this Order. To the extent production of source code becomes necessary in this case, the parties will work expeditiously to propose amendments to this Order to cover any production of source code.

16. If a party is served with a subpoena or a court order issued in other litigation that compels disclosure of any Confidential Information or Highly Confidential Information, the receiving party must:

(a) promptly notify in writing the designating party. Such notification shall include a copy of the subpoena or court order;

(b) promptly notify in writing the party who caused the subpoena or order to issue in the other litigation that some or all of the material covered by the subpoena or order is subject to this Stipulated Protective Order. Such notification shall include a copy of this Stipulated Protective Order; and

(c) cooperate with respect to all reasonable procedures sought to be pursued by the designating party whose Confidential Information or Highly Confidential Information may be affected.

If the designating party timely seeks a protective order, the party served with the subpoena or court order shall not produce any Confidential Information or Highly Confidential Information before a determination by the court from which the subpoena or order issued, unless the party has obtained the designating party's permission. The designating party shall bear the burden and

expense of seeking protection in that court of its confidential material—and nothing in these provisions should be construed as authorizing or encouraging a receiving party in this action to disobey a lawful directive from another court.

17. The following additional terms apply to non-party discovery material:

(a) The terms of this Order are applicable to information produced by a non-party in this action and designated as "CONFIDENTIAL" or "HIGHLY CONFIDENTIAL." Such information produced by non-parties in connection with this litigation is protected by the remedies and relief provided by this Order. Nothing in these provisions should be construed as prohibiting a non-party from seeking additional protections.

(b) In the event that a party is required, by a valid discovery request, to produce a non-party's confidential information in its possession, and the party is subject to an agreement with the non-party not to produce the non-party's confidential information, then the party shall:

i. promptly notify in writing the requesting party and the non-party that some or all of the information requested is subject to a confidentiality agreement with a non-party;

ii. promptly provide the non-party with a copy of the Stipulated Protective Order in this litigation, the relevant discovery request(s), and a reasonably specific description of the information requested; and

iii. make the information requested available for inspection by the non-party.

(c) If the non-party fails to object or seek a protective order from this Court within 28 days of receiving the notice and accompanying information, the receiving party may produce the non-party's confidential information responsive to the discovery request. If the non-party timely seeks a protective order, the receiving party shall not produce any information in its possession or control that is subject to the confidentiality agreement with the non-party before a determination by the Court. Absent a court order to the contrary, the non-party shall bear the

burden and expense of seeking protection in this Court of its Confidential Information or Highly Confidential Information.

18. Nothing in this Stipulated Protective Order shall be construed to preclude any party from asserting in good faith that certain Confidential Information or Highly Confidential Information requires additional protections. The parties shall meet and confer to agree upon the terms of such additional protection. By stipulating to the entry of this Protective Order no party waives any right it otherwise would have to object to disclosing or producing any information or item on any ground not addressed in this Stipulated Protective Order. Similarly, no party waives any right to object on any ground to use in evidence of any of the material covered by this Stipulated Protective Order. Nothing in this Stipulated Protective Order abridges the right of any person to seek its modification by the Court in the future.

Part Two: Use of Confidential Materials in Court

The following provisions govern the treatment of Confidential Information or Highly Confidential Information used at trial or submitted as a basis for adjudication of matters other than discovery motions or proceedings. These provisions are subject to Rules 2.550, 2.551, 2.580, 2.585, 8.160, and 8.490 of the California Rules of Court and must be construed in light of those Rules.

19. A party that files with the Court, or seeks to use at trial, materials designated as Confidential Information or Highly Confidential Information, and who seeks to have the record containing such information sealed, shall submit to the Court a motion or an application to seal, pursuant to California Rule of Court 2.551.

20. A party that files with the Court, or seeks to use at trial, materials designated as Confidential Information or Highly Confidential Information by anyone other than itself, and who does not seek to have the record containing such information sealed, shall comply with either of the following requirements:

(a) At least ten (10) business days prior to the filing or use of the Confidential Information or Highly Confidential Information, the submitting party shall give notice to all other parties, and to any non-party that designated the

materials as Confidential Information or Highly Confidential Information pursuant to this Order, of the submitting party's intention to file or use the Confidential Information or Highly Confidential Information, including specific identification of the Confidential Information or Highly Confidential Information. Any affected party or non-party may then file a motion to seal, pursuant to California Rule of Court 2.551(b); or

(b) At the time of filing or desiring to use the Confidential Information or Highly Confidential Information, the submitting party shall submit the materials pursuant to the lodging-under-seal provision of California Rule of Court 2.551(d). Any affected party or non-party may then file a motion to seal, pursuant to the California Rule of Court 2.551(b), within ten (10) business days after such lodging. Documents lodged pursuant to California Rule of Court 2.551(d) shall bear a legend stating that such materials shall be unsealed upon expiration of ten (10) business days, absent the filing of a motion to seal pursuant to Rule 2.551(b) or Court order.

21. In connection with a request to have materials sealed pursuant to Paragraph 12 or Paragraph 13, the requesting party's declaration pursuant to California Rule of Court 2.551(b)(1) shall contain sufficient particularity with respect to the particular Confidential Information or Highly Confidential Information and the basis for sealing to enable the Court to make the findings required by California Rule of Court 2.550(d).

IT IS SO STIPULATED.

DATED: _____, 2016

PERKINS COIE LLP

By: _____
Julie E. Schwartz

Attorneys for Defendant Facebook, Inc.

DATED: _____, 2016

BIRNBAUM & GODKIN, LLP

By: _____
David Godkin

Attorneys for Plaintiff
SIX4THREE, LLC

IT IS SO ORDERED.

DATED: 10/24, 2016

JUDGE OF THE SUPERIOR COURT

CERTIFICATION

I hereby certify my understanding that Confidential Information or Highly Confidential Information is being provided to me pursuant to the terms and restrictions of the Stipulation and Protective Order Regarding Confidential Information filed on October 25, 2016, in *Six4Three, LLC v. Facebook, Inc.*, San Mateo County Superior Court Case No. CIV533328 ("Order"). I have been given a copy of that Order and read it.

I agree to be bound by the Order and I understand and acknowledge that failure to so comply could expose me to sanctions and punishment in the nature of contempt. I will not reveal the Confidential Information or Highly Confidential Information to anyone, except as allowed by the Order. I will maintain all such Confidential Information or Highly Confidential Information, including copies, notes, or other transcriptions made therefrom, in a secure manner to prevent unauthorized access to it. No later than thirty (30) days after the conclusion of this action, I will return the Confidential Information or Highly Confidential Information, including copies, notes, or other transcriptions made therefrom, to the counsel who provided me with the Confidential Information or Highly Confidential Information. I hereby consent to the jurisdiction of the San Mateo County Superior Court for the purpose of enforcing the Order, even if such enforcement proceedings occur after termination of this action.

I hereby appoint Stuart G. Gross of Klein & Gross LLP located at the address of The Embarcadero, Pier 9, Suite 100, SF, CA 94111 as my California agent for service of process in connection with this action or any proceedings related to enforcement of this Stipulated Protective Order.

I declare under penalty of perjury that the foregoing is true and correct and that this certificate is executed this 14th day of May 2018 ~~2018~~, at Geneva, Switzerland.

By: Paul-Olivier Dehaye

Address: Chemin des Fauvettes 18
1212 Grand-Lancy

Phone: +41 76 407 57 96

The Big Read Technology sector

Data brokers: regulators try to rein in the 'privacy deathstars'

Companies that collect consumer information have operated in the shadows. But calls are growing for tougher rules

Aliya Ram and Madhumita Murgia in London JANUARY 8, 2019

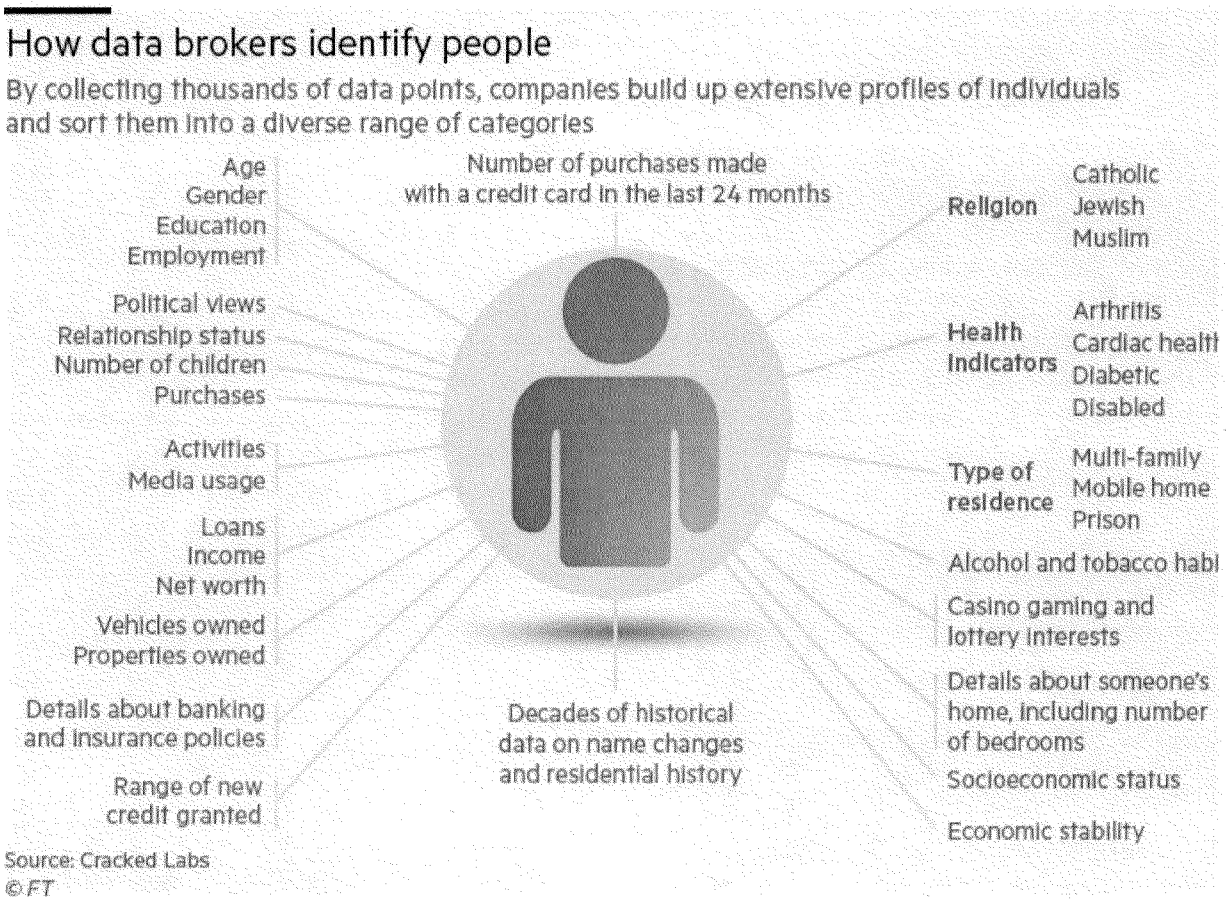
There are many personal details that Paul-Olivier Dehaye is willing to share online, but the behaviour of his bladder is not one of them. Yet when the Belgian privacy campaigner requested his data from advertising technology company Amobee, he found the business had predicted that on June 9 he was "likely to suffer from overactive bladder".

A legal representative for Amobee explained in an email to Mr Dehaye that the data had been licensed from The Weather Company, a business owned by technology group IBM. The Weather Company decided that based on hot weather conditions in Mr Dehaye's area he was likely to have an "overactive bladder" — and buy more drinks — on that day: "The overactive bladder [category] targets a mix of weather conditions that cause symptoms of overactive bladder to flare up, enabling advertisers to message when OAB is most likely to be top-of-mind for sufferers," the email said.

Few internet users will have heard of Amobee, a US company that sells advertising insights to the likes of Airbnb, Publicis and Lexus. But the business is just one of a constellation of adtech groups, data analytics firms and credit reference agencies that make up the rapidly growing data broking industry.

That industry is now very much in the regulatory spotlight in Europe. While the practices of its businesses have been investigated in the US for a number of years, regulators in Europe are now for the first time looking closely into their activities in the wake of the Cambridge Analytica data harvesting scandal last year and the introduction of the General Data Protection Regulation, Europe's new privacy law. Businesses that for years have operated largely in the shadows face the prospect this year of heightened scrutiny as public opinion shifts on questions of privacy.

The regulators have made it clear that they are deeply uneasy about the way the industry has been operating.

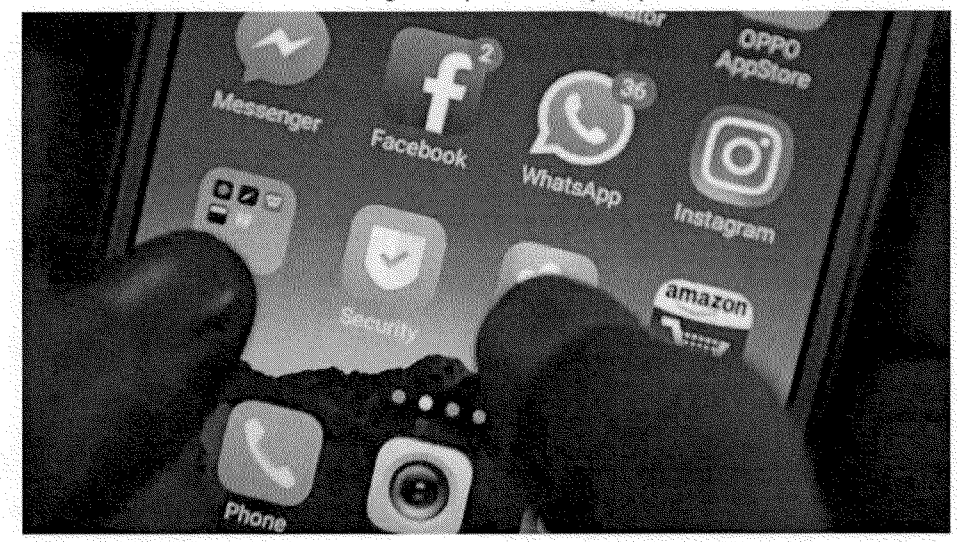


"They are all processing personal data, there is absolutely no doubt about that," says Mathias Moulin, director for the protection of rights and sanctions at the French data protection watchdog, CNIL. "They all try to say that it's anonymous to lower the pressure from the public, but that's not true. They know that and we know that."

While much of the attention last year focused on the use of data by tech groups such as Facebook, regulators and policymakers from the UK, France and Ireland who are examining the data-mining industry are turning their attention to the interlocking universe of lesser-known brokers that have also flourished as people spend more time online.

In November, Privacy International, the campaign group, asked European regulators to investigate seven brokers including software company Oracle after accusing them of breaking European data protection laws.

"[We are] concerned about whether or not their practices are compliant with the laws," says Elizabeth Denham, the UK's information commissioner. "We are looking at how they conduct their business and their general compliance with GDPR . . . certainly there is a dynamic tension between the way the businesses are conducted and the principles in the GDPR."



While much of the attention last year focused on the use of data by tech groups such as Facebook, regulators and policymakers are turning their attention to the interlocking universe of brokers © AFP

Data brokers mine a treasure trove of personal, locational and transactional data to paint a picture of an individual's life. Tastes in books or music, hobbies, dating preferences, political or religious leanings, and personality traits are all packaged and sold by data brokers to a range of industries, chiefly banks and insurers, retailers, telecoms, media companies and even governments. The European Commission forecasts the data market in Europe could be worth as much as €106.8bn by 2020.

"The explosive growth of online data has led to the emergence of the super data broker — the 'privacy deathstars', such as Oracle, Nielsen and Salesforce, that provide one-stop shopping for hundreds of different data points which can be added into a single person's file," says Jeffrey Chester, executive director of the Center for Digital Democracy based in Washington. "As a result, everyone now is invisibly attached to a living, breathing database that tracks their every move."

Over the past five years, the data broker industry expanded aggressively in what amounted to a virtual regulatory vacuum. The rise of internet-connected devices has fuelled an enhanced industry of "cross-device tracking" that matches people's data collected from across their smartphones, tablets, televisions and other connected devices. It can also connect people's behaviours in the real world with what they are doing online.

"The dream for the industry is to be able to connect the online and offline worlds to have a 360-degree view of the customer," says Gabriel Voisin, partner in international privacy and data protection at Bird & Bird, the law firm.

In November, Privacy International, the campaign group, asked European regulators to investigate seven brokers including software company Oracle after accusing them of breaking European data protection laws © Bloomberg

While brokers do not ever buy data directly from consumers, they are central to the data market. Even consumer data leaders such as Facebook, Google, Twitter and Snapchat have signed up as customers of brokers such as Acxiom, Oracle, Experian and others, because of the wealth and granularity of offline and cross-device data they have accumulated. For instance, if you went into a supermarket and bought baby wipes or nappies, that information could land you on a list for showing targeted ads to new parents.

According to IDC analyst Karsten Weide, growing demand should cause data vendor sales to more than triple to $10.1bn by 2022, compared with $3.1bn in 2017.

"The large platform giants, Google, Facebook and a few others — they are the major nodes in today's personal data economy," says Wolfie Christl, a researcher at Cracked Labs, a non-profit group based in Austria. "At the same time there is a kind of distributed surveillance economy . . . [that is] also collaborating with each other and large old-school data brokers like Acxiom."

Facebook chief Mark Zuckerberg at a US Senate hearing. Consumer data leaders such as Facebook have signed up as customers of brokers such as Acxiom, Oracle, Experian and others, because of the wealth and granularity of offline and cross-device data they have accumulated © AFP

One of the largest data marketplaces is Oracle, the computer software company based in California. Oracle owns and works with more than 80 data brokers who funnel in an ocean of data from their own range of sources, including consumer shopping behaviour at brick-and-mortar stores,

financial transactions, social media behaviours and demographic information. The company claims to sell data on more than 300m people globally, with 30,000 data attributes per individual, covering "over 80 per cent of the entire US internet population at your fingertips".

Richard Petley, head of Oracle in the UK, told the FT in August that there was "lots of opportunity" in data analytics as people spend more time online. Oracle declined to comment for this article.

Others, such as credit rating agency Experian and Acxiom use demographic, sociographic, lifestyle, cultural, mortgage and property data to categorise individuals. Experian uses the "Asian heritage" label for targeting "large extended families in neighbourhoods with a strong South Asian tradition", while Bank of Mum and Dad describes households where a grown-up child still lives at home.

Best known for its consumer credit scores, Experian's business model has changed significantly since it went public over a decade ago. Its data business comprises 55 per cent of its revenues, with the rest coming from other services such as identifying fraud or helping customers make credit decisions.

Under the company's "One Experian" transformation plan announced last year, it has sought to "connect different data sources", according to its annual report. By law, the company cannot sell data collected for credit decisions to advertising customers,but according to chief executive Brian Cassin, the businesses overlap "to a degree" as the company seeks "to build much more precise products" that use data to build more accurate tools for predicting credit worthiness, affordability and the likelihood of fraud.

Despite the sensitive nature of the data that brokers gather, acquiring the information they compile can be surprisingly easy. In October, Spanish researcher Joana Moll was able to buy the online dating profiles of 1m people for €136 from data broker USDate. The profiles of unsuspecting customers, garnered from online dating app Plenty Of Fish, included 5m photographs and details like their date of birth, zip code and gender as well as intimate information like sexuality, religion, marital status and whether they smoke, drink or have children. Plenty of Fish says it does not sell user data to USDate, and was unclear about the provenance of this data set.

"It's really easy, it was like buying a T-shirt on Amazon, and you can buy it anywhere in the world," Ms Moll says. "We acquired a second batch two weeks ago to see if anything had changed after GDPR but nothing had, we got the same number of profiles."

Alexander Nix, CEO of Cambridge Analytica © Reuters

Data brokers in the US have been scrutinised by lawmakers for more than two decades, but they have never been subject to any federal oversight. The last time the industry faced close inspection was in 2014 when the US Federal Trade Commission produced a 110-page report compiled over two years on nine of the biggest data brokers, including Acxiom and Datalogix, bought by Oracle at the end of that year. The commission recommended strongly that Congress introduce legislation to limit the reach of brokers, but versions of this draft legislation are still being kicked around on Capitol Hill today.

In Europe, pressure has built as investigations were launched into the industry. In the aftermath of the Cambridge Analytica scandal, the UK Information Commissioner's Office issued assessment notices to Acxiom, Data Locator Group and GB Group as well as Experian, Equifax and Callcredit, allowing it to carry out compulsory audits. CNIL, the French data protection authority, has carried out more than 50 inspections of data brokers and adtech companies in the past two years, including Paris-based Criteo.

Data brokers insist they comply with local laws by keeping consumers' identities anonymous; instead, they compile information on people's locations, shopping habits and browsing behaviour using pseudonymous identifiers or aggregated information. According to Amobee and IBM, for example, the overactive bladder category is not based on health information, but uses the weather in a particular area to predict whether people might be more likely to buy beer or water. Amobee added that it never used the data to send targeted ads.

IBM did not reply to requests about whether the predictions were based on location data but said the category "allows an advertiser to know when the weather in a certain location is potentially suitable for overactive bladder to occur". The Weather Company is currently facing a lawsuit from the city attorney of Los Angeles for "deceptively [using] its Weather channel app to amass its users' private, personal geolocation data". IBM has said The Weather Company has always been transparent about its use of location data.

Elizabeth Denham, the UK's information commissioner: 'We are looking at how [data brokers] conduct their business and their general compliance with GDPR' © Jon Super/FT

Critics say brokers are misleading people by claiming the data are truly anonymous. "None of these actors are processing anonymous data; they are processing personal data," says Mr Moulin at the CNIL. "Data on location is very sensitive, with data on location you can identify a natural [real] person."

Other regulators say businesses could fall foul of GDPR if sensitive data can be inferred from these audience categories. The European rules set higher standards for any data revealing categories such as "racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership".

"We will be asking organisations to justify if they have [audience] names that suggest a special category [of] data," says a senior official at one European data protection regulator, which is examining the industry.

Data brokers are already starting to make organisational changes. "When GDPR came in, people were forced to look at the legislation and realised the tech they were using was right at the boundary and limit of the existing [law]," says John Mitchison, head of policy and compliance at the Data & Marketing Association, the trade body for data-driven businesses.

"One of the most drastic things I've seen happen is all of these companies have radically reduced the number of third-party companies they will accept data from. You now need evidence that data were collected properly so they've weeded out a lot of suppliers that don't meet those standards."

CallCredit, one of the major credit reference agencies, which also had a big marketing data file, took a product off the market completely, and was subsequently taken over by TransUnion, a US company. Meanwhile Acxiom sold off its business, now called LiveRamp, that offers more controversial "identity resolution" services that link disparate atoms of data to create a profile of an individual, although it still accesses some of these services as a customer of LiveRamp.

Industry executives are hoping that these measures will fend off a much tougher assault on their business model from anxious regulators.

Additional reporting by Camilla Hodgson

Letters in response to this article:

GDPR should help expose violations of consent / From Stephen Wright, London, UK

Data harvesting in the days of direct mail / From Marco Bueninck, Mexico City, Mexico

Latest on Technology sector

Follow the topics in this article

US & Canadian companies

Digital politics

Technology sector

EU tech regulation

Cambridge Analytica